NPS-CS-08-010

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

A Testbed for High Assurance and Dynamic Security

by

Thuy D. Nguyen, Cynthia E. Irvine, Timothy E. Levin

19 May 2008

Approved for public release; distribution is unlimited

Prepared for: Office of Naval Research and the National Reconnaissance Office

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

This material is based upon work supported in part by the Office of Naval Research and the National Reconnaissance Office.

This report was prepared by:

_____
Thuy D. Nguyen
Research Associate of Computer Science

Reviewed by:

_____
Peter J. Denning, Chair
Department of Computer Science

Released by:

_____
Dan C. Boger
Interim Vice President and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** May 2008	**3. REPORT TYPE AND DATES COVERED** Technical Report	
4. TITLE AND SUBTITLE: A Testbed for High Assurance and Dynamic Security			**5. FUNDING NUMBERS**
6. AUTHOR(S) Thuy D. Nguyen, Cynthia E. Irvine, Timothy E. Levin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-CS-08-010
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Naval Research National Reconnaissance Office			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Providing a stable testing environment for experimentation is a common goal of all Testbeds. To date, few, if any, have supported research in high assurance multilevel security (MLS), cross domain enterprise services and emerging Information Assurance technologies envisioned for the Global Information Grid and similar complex distributed enterprise networks. To facilitate this research, an MLS Testbed has been developed to support experimentation on, rapid prototyping of, and testing of the results of selected MLS technologies. The MLS Testbed integrates a variety of multi-vendor equipment and software to simulate a realistic network with dynamic and collaborative operational needs. This report describes the design of the MLS Testbed, the MYSEA MLS architecture and recent enhancements to the MYSEA software architecture to support IPsec-based dynamic security services.

14. SUBJECT TERMS Multilevel security, testbed, high assurance, dynamic security, Monterey Security Architecture (MYSEA)			**15. NUMBER OF PAGES** 23
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-CS-08-010

The Center for Information Systems
Security Studies and Research

Technical Report

A Testbed for High Assurance and Dynamic Security

Thuy D. Nguyen, Cynthia E. Irvine, Timothy E. Levin

May 19, 2008

Acknowledgements

This work was sponsored in part by the Office of Naval Research and the National Reconnaissance Office. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Office of Naval Research, the National Reconnaissance Office or Naval Postgraduate School.

The authors would like to thank David Shifflett, Jean Khosalim, Paul Clark, Charles Prince and Philip Hopfner who contributed to the evolution of this Testbed.

Author Affiliation

Center for Information Systems Security Studies and Research
Department of Computer Science
Naval Postgraduate School
Monterey, California 93943
U.S.A

Abstract

Providing a stable testing environment for experimentation is a common goal of all Testbeds. To date, few, if any, have supported research in high assurance multilevel security (MLS), cross domain enterprise services and emerging Information Assurance technologies envisioned for the Global Information Grid and similar complex distributed enterprise networks. To facilitate this research, an MLS Testbed has been developed to support experimentation on, rapid prototyping of, and testing of the results of selected MLS technologies. The MLS Testbed integrates a variety of multi-vendor equipment and software to simulate a realistic network with dynamic and collaborative operational needs. This report describes the design of the MLS Testbed, the MYSEA MLS architecture and recent enhancements to the MYSEA software architecture to support IPsec-based dynamic security services.

Table of Contents

1. Introduction

The technical vision of the emerging net-centric Global Information Grid (GIG) [1] encompasses support for high assurance user and component authentication and multilevel security (MLS) as well as flexible, dynamic security policies. The GIG is intended to address the inefficient exchange of information in current military and intelligence operations that utilize a variety of specialized ("stove-piped") computing and communications systems while maintaining requisite security controls. Secure information access problems are exacerbated by the need to share information from networks at different classifications and within multinational coalitions in dynamic, ad hoc situations. MLS systems can support controlled sharing of information based on both its integrity and confidentiality attributes, and are applicable to non-military environments such as state and local governments, and large commercial enterprises.

Another challenge that must be addressed in practical systems is the efficiency and user-driven requirement for access to commodity software familiar to many users, but which lacks robustness and meaningful security protections. Without sufficient security measures and mechanisms, the realization of a useable and defensible information infrastructure may be only a chimera.

The research and integration challenges of high assurance multilevel security with dynamic services provide the impetus for three synergistic research efforts: the Monterey Security Architecture (MYSEA) project [2], the Trusted Computing Exemplar (TCX) project [3, 4] and the Dynamic Security Service (DSS) project. The MLS Testbed provides a controlled environment to assess experimental results of these projects, explore other new technologies, showcase demonstration prototypes and support student research. The MYSEA and DSS projects are more mature than the TCX project, and thus, current Testbed experiments are primarily MYSEA- and DSS-related.

This report describes the design of the MLS Testbed, the MYSEA MLS architecture and some of the on-going MYSEA experiments. The GIG vision anchors our research activities, but any extended, rapidly evolving enterprise with information assets having a range of value and criticality as well as a range of users with different authorizations will also have similar requirements.

2. Background

Strong and secure authentication is an important IA enabler for the GIG vision [1]. High assurance Identification and Authentication (I&A) mechanisms afford a high level of confidence in accountability of participants and support single sign-on capabilities required in complex and dynamic environments. High assurance I&A [5] requires users to have a positive connection to trusted system elements that provides confidence that neither the system nor the user is being spoofed. This connection is known as a trusted path.

MYSEA is a distributed operating environment capable of enforcing multilevel security policies while maintaining support for new and legacy applications and unmodified commodity client systems. The architecture supports protocols and equipment from a wide range of vendors as well as secure interaction with external classified networks.

The purpose of the TCX project is to provide an openly distributed worked example of how high assurance trusted components can be constructed. As a reference implementation, the TCX Least Privilege Separation Kernel (LPSK) is being developed in accordance with the Common Criteria evaluation methodology [6] at Evaluation Assurance Level 7 (EAL 7). It will also be in compliance with the EAL6+ Separation Kernel Protection Profile. [7] The LPSK will be used as the underlying trusted foundation for two trusted components used in MYSEA: the Trusted Path Extension (TPE) and Trusted Channel Module (TCM). The former will constitute a reference "trusted application" for the TCX project and is being constructed to be evaluatable at EAL6.

Another key IA enabler for assured information sharing in the GIG is the dynamic security paradigm under which access control decisions are based on a number of factors, including: data sensitivity, security risks, and operational needs [1]. Our previous work in adaptive security [8] extended the traditional Quality of Service paradigm beyond just network and performance attributes to include security as a multidimensional resource that could be dynamically controlled. By providing users and the underlying resource management mechanisms with control over levels of security service and associated resource usage, security could be transformed from a performance obstacle into a constructive network management tool. For example, integration of network management and status detection functions with underlying security service modulation functions allows a distributed system to dynamically adapt its communication security posture to resource and policy changes. The Dynamic Security Service (DSS) project is building on the previous work by exploring how dynamic modulation of security services can be integrated into an MLS environment and how those services can be expanded to support the sorts of flexible security policy envisioned for the GIG.

3. Testbed Design

The primary objective of the MLS Testbed is to provide an evolving research and development facility capable of supporting different research projects, including those of students and collaborators from other institutions. Figure 1 is a notional diagram of the Testbed architecture.

The MLS Testbed is comprised of several disconnected network "segments" and spans multiple physical locations. The Demonstration Segment showcases the MYSEA distributed MLS environment as described below.

The Development Segment consists of separate "mini-networks" that are used to explore new ideas or to develop rapid prototypes. In contrast with the relatively static Demonstration Segment, the hardware and software configurations of the mini-networks are ephemeral and loosely managed, i.e., each mini-network is individually maintained by a lead researcher. The mini-networks utilize the VMWare virtualization software to optimize equipment sharing. This

segment currently supports MYSEA-related Voice-over-IP and IPv6 research, the development of a functional prototype of the TCX LPSK, and other MLS experiments.

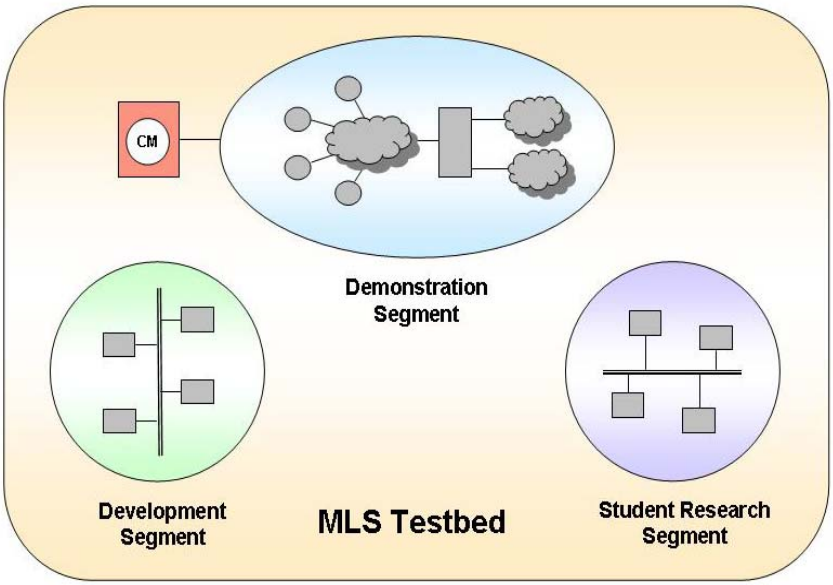

Figure 1. MYSEA MLS Testbed Architecture

Similarly, the Student Research Segment consists of separate mini-networks that are assigned to Masters and Ph.D. students. The mini-networks supporting student research are typically smaller in scale and simpler in scope than those of the Development Segment. Again, VMWare is used to minimize the hardware footprint of the experiments.

As with all tests and experiments, control of configuration and environmental variables that could affect the outcome is important. This requires a detailed record of the exact configuration of the Demonstration Segment, including topology, and versions of hardware, firmware and software. A strict life cycle process has been in place to control the administration and operation of the Testbed since its inception. Only authorized personnel are granted access to the Testbed, and only stable software releases may be installed on the Demonstration Segment. Before any hardware or software element is incorporated or upgraded, unit and regression testing verify that each element works properly.

4. MYSEA Overview

The MYSEA network architecture affords users the ability to securely access information across networks at different classifications using unmodified commodity applications. In MYSEA, highly trustworthy MLS servers provide the locus of security policy enforcement, while highly trustworthy appliances, specifically the TPE and TCM, ensure unspoofable authentication of users and single level networks, respectively. Other system components provide the users the ability to run unmodified office productivity tools and DoD applications, as illustrated in Figure 2. Although not shown as a LAN in Figure 2, the “white pipes” shown on the left of the MLS

servers constitute an MLS LAN wherein different sessions operating at different security levels can exist at a given time. An instance of this network architecture is currently implemented in the Testbed's Demonstration Segment.

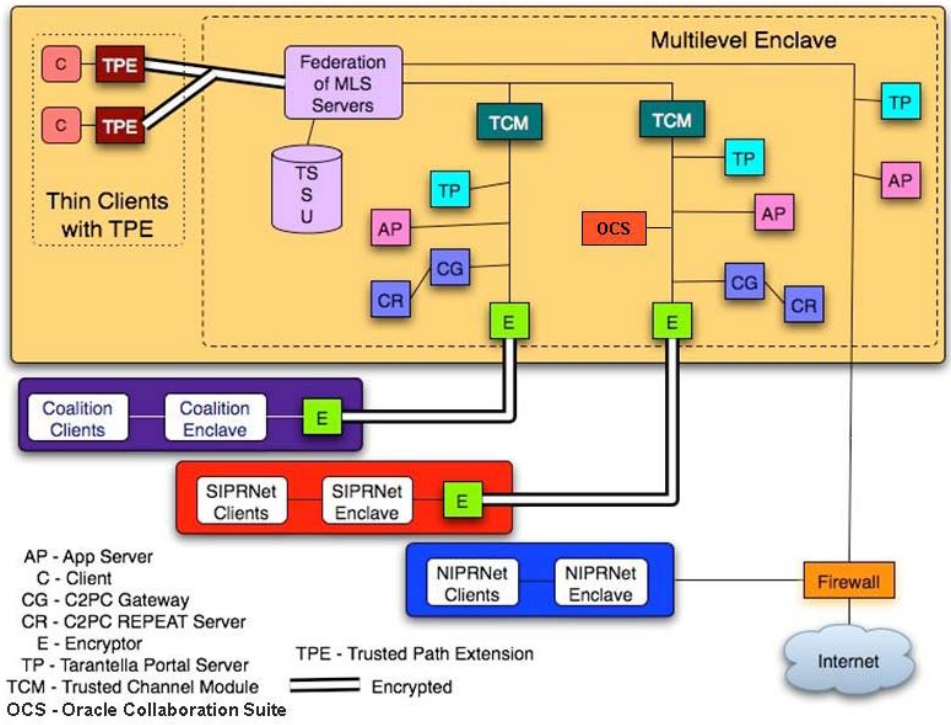

Figure 2. Monterey Security Architecture

The MYSEA MLS network architecture is designed to support:

- Secure connections to classified networks
- Use of commercial-off-the-shelf (COTS) and legacy hardware and software components
- Use of open standards
- Centralized security management
- Use of adaptive security techniques to provide dynamic security services
- Integration of high assurance multilevel security with existing sensitive networks
- High assurance trusted communication channels to classified networks
- Open interfaces to incorporate new technologies
- Use of XML tags as security markings
- Secure single sign-on across multiple MLS servers
- Server cluster technologies
- IPv6 in a multilevel context

A federation of MLS servers within the Testbed enforces a unified mandatory access control security policy based on the Bell and LaPadula [9] confidentiality policy and the Biba [10] integrity policy. A challenging problem has been the lack of a high performance, easy-to-use, high assurance MLS server platform. Several Unix-based MLS platforms such as SELinux, Trusted Solaris, Policy-Enhanced Linux [11], and Policy-Enhanced OpenBSD [12] were not considered due their lack of high assurance. The BAE XTS-400, a certified MLS platform [13], was selected as the underlying trusted foundation for the MYSEA server. Although the XTS-400 STOP OS (Version 6) provides higher assurance than the others, it does not provide an MLS network interface and TCP/IP stack, remote trusted path, remote file system, or remote interactive shell capability. Therefore, the MYSEA project developed custom software (both trusted and untrusted) necessary to create a useable MLS LAN environment. New functionalities such as support for MLS network interfaces and IPsec-enabled TCP/IP stack have been announced for a future STOP OS release and we are studying these enhancements to determine if and how they can be effectively used in MYSEA.

The Trusted Path Extension (TPE) device is responsible for providing a secure interface for user interaction with trusted services on the MLS server. After a successful login and session level negotiation via the TPE, an MLS LAN user can use their client workstation to access data on the MLS server which is authorized for that level. As enforced by the MLS server, MYSEA allows reading information that is at the same or lower in sensitivity than the negotiated session level. All information written will be labeled at the negotiated session level. Similarly, the Trusted Channel Module (TCM) device is a trusted component responsible for providing secure identification of single level networks connected to the MLS server. Users on these networks can only access data on the MLS server at the classification level of the single level network from which they are operating.

The use of a single client workstation for cross-domain access provides a dramatic physical footprint reduction compared to other approaches. However, without appropriate security measures, use of a single workstation magnifies the risk of information leakage between sessions at different security levels. In particular, residual information in memory or other internal components of the workstation allocated during a high session may not be properly purged prior to the reallocation of the reallocation of those resources during a low session. To address these object reuse issues, the MYSEA approach is to use “stateless” clients. All persistent user data and metadata associated with a session at a particular sensitivity level are stored on the MLS server at that sensitivity level rather than on the workstation. To avoid object reuse, our current solution is to recycle power at the workstation whenever a transition to a less sensitive session takes place, and alternative techniques are the subject of ongoing research.

The Tarantella Enterprise 3 servers on the single level networks, acting as application-level gateways, provide MLS LAN clients the ability to access remote server-based applications through a Java-enabled web browser. The Tarantella server allows an authenticated user to interact with a remote application as if the application ran locally on the client. Through the Tarantella virtual desktop (i.e., WebTop), the user can securely use proprietary applications on the simulated legacy networks, e.g., Word and PowerPoint.

The Oracle Collaboration Suite (OCS) provides a distributed application environment based on the emerging Service Oriented Architecture (SOA). A user logged in at Secret can access services such as email and WebDAV file browser on the OCS server on the simulated Secret network. We plan to continue to investigate the effective use of MLS technology in SOA-based environments.

5. MYSEA Software Architecture

The MYSEA software architecture is illustrated in Figure 3. The MLS server, the TPE and the TCM consist of a high assurance computing foundation (diagonal shading), i.e., TCX LPSK and STOP OS, the Protected Communications Service (PCS) component and the DSS components (cross-hatched shading). The PCS component provides IPsec-based protected communication channels between the TPE and server, and between the TCM and the server. The DSS components implement a dynamic service management mechanism that can adjust to resource and policy changes thus adapting to changing operational needs and threats as envisioned for the GIG.

The Trusted Path Service (TPS) and Trusted Path Application (TPA) components together enforce the identification and authentication supporting policy to ensure that only authorized users can gain access to the server. The TPA affords the users unspoofable access to security-critical services and is invoked via a Secure Attention Key. The TPS component on the server handles user authentication and session negotiation functions. Likewise, the Trusted Channel Service (TCS) and the Trusted Channel Application (TCA) components ensure that traffic between a single level network and the MLS server are properly labeled at the classification level of the particular network.

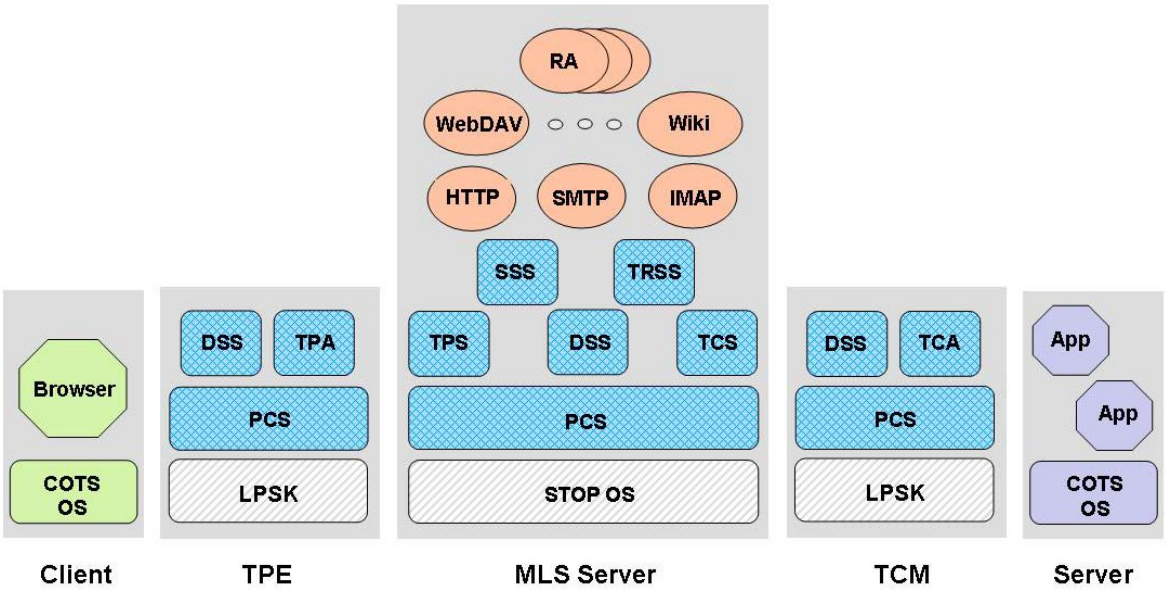

Figure 3. MYSEA Software Architecture

The Secure Session Service (SSS) component and the application protocol servers, e.g., HTPP server, are responsible for handling server application requests from the clients. The SSS ensures that each request is associated with a valid user session prior to spawning the corresponding application server to process the application-specific functions. This prevents the indiscriminate launch of application services and ensures that all services are associated with the correct sensitivity level and user. Because the application servers run at the users' session levels, they must rely on the SSS to perform network operations on its behalf. The MLS server also includes a number of MLS-aware application services such as Wiki and email (SMTP, IMAP).

Support has also been developed on the MLS server for a client to remotely execute a client application on the server. This capability is necessary because certain clients may be configured to only run a browser locally. Similar to the application servers, the Remote Application (RA) component, e.g., a TFTP client, runs at the user's session level and depends on the Trusted Remote Session Service (TRSS) component to perform network operations on MLS interfaces on its behalf. If a RA attempts to communicate with a remote server, the TRSS checks the security levels of the RA and the remote server to ensure that the MLS policy is not bypassed.

6. MYSEA Demonstration Network

The MYSEA demonstration network is an instantiation of the MYSEA architecture. It resides in the Testbed's Demonstration Segment and hosts a number of demonstrations that include popular desktop applications, e.g., the Microsoft Office suite, for providing access to data at different classification levels. For example, a U.S. user on the MLS LAN can log in at a given security level from the same client workstation to view information stored on the MLS server that is at or below that level.

A Linux-based functional prototype TPE is used while work is progressing on the TCX LPSK. The TCM is not yet incorporated in the demonstration, so simulated Secret and Coalition networks (shown in Figure 2) are separately connected to the MYSEA server via two single level network interfaces. Thus, instead of multiplexing these connections through a single MLS component, separate physical connections ensure isolation.

Both Knoppix and Windows XP Embedded thin clients run on the client workstation. Preliminary performance measurements indicate no visible performance difference between these platforms for retrieving data (as measured by throughputs), either directly from the MYSEA server or indirectly from backend servers through Tarantella. However, it takes somewhat longer for the Tarantella WebTop to initially come up on the Windows thin client. The Tarantella server software currently used in the Testbed requires a custom Java applet on the client, and thus, it is hypothesized that this behavior is a side effect of the Java Virtual Machine and Java applet initialization functions.

The security services that currently are implemented in the demonstration can be grouped into four categories: MLS services, single level services, transmission security services and controlled Internet access.

6.1 MLS Services

The MYSEA server is currently configured to run an Apache-like (modified Apache) web server that supports WebDAV and Wiki services, and modified sendmail and imapd mail servers. After a successful login to the MYSEA server at an authorized session level via a TPE-enabled client, a user on the MLS LAN can view web pages at the same or lower sensitivity level; use WebDAV to create, edit and manage files kept on the MLS data store; or access a policy-constrained wiki. The user can also exchange email with other users who are logged in at the same session level, and can read previously-received email from lower sensitivity levels.

6.2 Single Level Services

The following COTS applications have been tested and are being used in the demonstration via the Tarantella integrated portal interface: Microsoft Office (Word, PowerPoint, Excel, Access), Microsoft Project and Microsoft Outlook Express.

The Command and Control Personal Computer (C2PC) system, a battlefield situational awareness tool, demonstrates the ability to support mission-critical applications. The C2PC REPEAT system simulates a Global Command and Control System (GCCS) server that generates tactical information. The C2PC Gateway receives the stream of tracking data and relays it to the C2PC Clients, and also forwards track updates from the C2PC Clients to the GCCS server. In the demonstration, the C2PC Client is a Windows application hosted on an MLS LAN client workstation, which displays the tactical map window.

6.3 Transmission Security Services

Two pairs of high assurance military network encryptors, TACLANEs, are used to simulate encrypted channels required for classified transmissions across a WAN, i.e., between the MYSEA controlled environment and the simulated Secret and Coalition networks. In the unclassified Testbed environment, the TACLANE devices are keyed with unclassified test keys. Two pairs of Cisco IPsec VPN devices are also used for testing encrypted channels.

6.4 Controlled Internet Access

There are two ways that a user on the MLS LAN can access the Internet. One is through a dedicated network interface on the MYSEA server operating at the lowest classification which is not shown in Figure 2; the other is through the Internet gateway in the simulated Unclassified network. In both cases, the web server application running on the MYSEA server acts as a proxy web server for HTTP requests originating from the MLS LAN client.

7. Conclusion

The design of the MLS Testbed was started in 2004 and has evolved to support a wide variety of services and applications. The Testbed is divided into different segments to provide both a controlled environment to demonstrate mature research results such as those of the MYSEA project and an adaptive environment to conduct research and experimentation on emerging technologies and MLS solutions.

References

1. IA Architecture Office (I11), "Global Information Grid Information Assurance Capability/Technology Roadmap", Version 1.0, National Security Agency Information Assurance Directorate, April 2005.

2. Irvine, C. E., Levin, T. E., Nguyen, T. D., Shifflett, D., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J., "Overview of a High Assurance Architecture for Distributed Multilevel Security," Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004, pp. 38-45.

3. Irvine, C. E., Levin, T. E., Nguyen, T. D., and Dinolt, G. W., "The Trusted Computing Exemplar Project," Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004, pp. 109-115.

4. Nguyen, T. D., Levin, T. E., and Irvine, C. E., "TCX Project: High Assurance for Secure Embedded Systems," 11th IEEE Real-Time and Embedded Technology and Applications Symposium Work-In-Progress Session, San Francisco, CA, March 2005.

5. Common Criteria Project Sponsoring Organizations, "Common Criteria for Information Technology Security Evaluation," Parts 1-3, Version 3.1 Revision 2, September 2007.

6. Common Criteria Project Sponsoring Organizations, "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements," CCIMB-2005-08-003, Version 2.3, August 2005.

7. National Security Agency, "U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness," Version 1.03, 29 June 2007.

8. Levin, T. E., Irvine, C. E., and Spyropoulou, E., "Quality of Security Service: Adaptive Security," Handbook of Information Security, Vol.3, pp 1016-1025, ed. H. Bidgoli, John Wiley and Sons, 2006.

9. Bell, D. E. and LaPadula, L., "Secure Computer System: Unified Exposition and Multics Interpretation," Tech. Rep. ESD-TR-75-306, MITRE Corp., Hanscom AFB, MA, 1975.

10. Biba, K. J., "Integrity Considerations for Secure Computer Systems," Tech. Rep. ESD-TR-76-372, MITRE Corp., 1997.

11. Clark, P. C., "Policy-Enhanced Linux," Proceedings of the 23rd National Information Systems Security Conference, Baltimore, MD, October, 2000, pp. 418-432.

12. Nguyen, T. D., and Levin, T. E., "Policy Enforced Remote Login," NPS Technical Report NPS-CS-03-004, February 2003.

13. BAE Systems Information Technology, LLC, “Security Target, Version 1.11 for XTS-400 Version 6,” December 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library, Code 013 Naval Postgraduate School Monterey, CA 93943-5100	2
3.	Research Office, Code 09 Naval Postgraduate School Monterey, CA 93943-5138	1
4.	Dr. John Monastra Aerospace Corporation Chantilly, VA	1
5.	Dr. Ralph Wachter Office of Naval Research Arlington, VA	1
6.	Dr. Cynthia E. Irvine Code CS/Ic Department of Computer Science Naval Postgraduate School Monterey, CA 93943	1
7.	Timothy E. Levin Code CS/Tl Department of Computer Science Naval Postgraduate School Monterey, CA 93943	1
8.	Thuy D. Nguyen Code CS/Tn Department of Computer Science Naval Postgraduate School Monterey, CA 93943	1